

Back-
ground

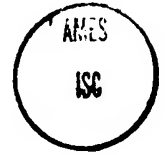
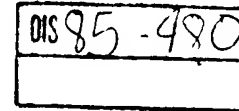


General
Service
Administration

Information Security
Oversight
Office

Washington, DC 20405

September 3, 1985



03 SEP 1985

STAT

[Redacted]
Director, Office of
Information Services
Central Intelligence Agency
Washington, DC 20505

Dear [Redacted]

STAT

We enclose for your review and comment the papers submitted by the five task forces on information security initiatives established at the interagency meeting of July 30, 1985. As agreed at that meeting, comments are due at ISOO by September 27, 1985, so that they may be distributed to the participating agencies by October 1. Your comments may include recommendations for alternative initiatives that have not been included by the task force. Feel free to include comments on any task force paper, even the task force on which your agency served. ISOO will also include its comments in the package to be circulated by October 1. The format of your comments should clearly identify the particular task force, e.g., overclassification, the particular initiative, and your evaluation of it, with respect to both the substance of the initiative and the recommended means of implementation.

We are most appreciative of the effort and thought that has gone into these recommended initiatives. We ask that this commitment continue, as we work toward the improvement of the information security system.

Sincerely,

STEVEN GARFINKEL
Director

Enclosures

TASK FORCE PAPER
INFORMATION SECURITY INITIATIVES
UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

Purpose

This report is a presentation of recommendations to reduce the number of unauthorized disclosures of classified information. Procedures for implementing these initiatives also are presented in the report.

Discussion

Leaks, i.e., unauthorized disclosures of classified information, at a minimum, are eroding the nation's capability to conduct its foreign relations and are making the national defense more costly. As used in this paper, an unauthorized disclosure refers only to deliberately revealing classified information, to one or more persons not authorized to have access to that information, for an intent other than committing espionage.

In one context, the problem centers around the relatively miniscule number of leakers when compared to the over four million persons having access to classified information. Because of the widely held belief that those leaking classified information are never punished, some individuals feel free to reveal classified information to support their personal opinions.

Many of the so called leaks are friendly or intentional disclosures of classified information by senior policy officials that are designed to support an administration's position. These leaks undermine confidence in the classification system and make it even more difficult to prosecute unauthorized disclosure cases.

Background

The establishment of efforts to control leaks goes back to at least the Eisenhower Administration, with the number of leaks and the problems of controlling them expanding greatly during the intervening years. The most recent and relevant study on the leak phenomenon is the March 1982 "Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information." The study's recommendations were endorsed by the Attorney General and most of them were implemented by National Security Decision Directive (NSDD) Number 84 entitled "Safeguarding National Security Information" dated March 11, 1983. However, many requirements of this NSDD have been controversial.

Because of the completeness of the above Report, several of its recommendations pertaining to NSDD 84 have been included in this paper by the Task Force.

LIMITED OFFICIAL USE

Initiative

Identify proposed legislation/regulations concerning the implementation of NSDD 84 sections that impact on unauthorized disclosures and take appropriate actions.

- o Enforcement of NSDD 84 requirements not held in abeyance by Congressional action should be a high priority in controlling leaks. The imposing of administrative sanctions and withdrawals of access, regardless of level of the individual, should be the norm not the exception in those leak cases where the leaker is identified. It is recommended that agency Standards of Conduct be invoked and the applicable penalties authorized in leak cases. It also is recommended that there be a minimum penalty for all individuals found to be leakers. The penalty would be part of the Standards of Conduct and would be other than a verbal reprimand.
- o In March 1985, a decision was made by the Office of Management and Budget (OMB) at a meeting of the key agencies and departments, that senior policy makers would have to make a determination as to what type of legislation, if any, should be proposed to Congress pertaining to unauthorized disclosures. It is recommended that this determination be made.
- o The NSDD 84 requirement for a study of the Federal personnel security program has not been completed. The study group, chaired by the Department of Justice (DOJ), submitted a paper to the National Security Counsel (NSC) more than a year ago seeking guidance on four fundamental issues. It is recommended that these questions be answered by the NSC to allow completion of this requirement.
- o The NSDD 84 requirement for development of procedures permitting the use of polygraphs on leak investigations has been suspended by the President following Congressional criticism of the proposal. It is recommended that policy makers revisit this issue in an effort to develop a more narrow but more politically acceptable polygraph policy.

Implementation

The Task Force recommends that Information Security Oversight Office (ISOO) take the lead in raising these issues with the NSC staff.

LIMITED OFFICIAL USE

Initiative

Develop educational media concerning unauthorized disclosures to increase awareness among Government employees, in particular political appointees and senior policy makers.

- o Establish a requirement for including in security briefings, for at least newly cleared employees, information on the responsibilities of Government employees pertaining to unauthorized disclosures. It is recommended that material be included in existing briefings on procedures dealing with the media and the damage done by leaks. In addition, it is recommended that all cleared employees be given a security handbook emphasizing their duty to protect classified information and the proper ways to have information declassified for release to the public.
- o Production of educational material, both classified and unclassified, is the foundation of any program to control unauthorized disclosures. It is recommended that the several proposals by the Central Intelligence Agency (CIA) for classified videotapes on leaks be completed as soon as practical with particular emphasis on briefing materials for senior policy makers. Further, it is recommended that damage report training materials, both videotapes and printed, with unclassified examples of the harm done to the national security by leakers be produced for uncleared Government employees and the public at large.

Implementation

Since these recommendations encompass the entire Federal Government, the Task Force suggests that ISOO take the lead in developing proposals for the unclassified materials. In addition, the CIA should be advised by ISOO of these recommendations of the Task Force.

LIMITED OFFICIAL USE

Initiative

Develop programs to encourage the reporting of unauthorized disclosures e.g., set up a toll-free hotline and also an incentives program offering rewards or awards for reporting "leakers" or potential leaks.

- o The Department of Defense (DOD) has established a "hotline" for reporting various types of security information. Also, the CIA has discussed initiating a proposal to establish rewards for reporting unauthorized disclosures of classified information. It is recommended that ISOO review the current hotline effort and rewards suggestion to determine the feasibility of these procedures for the remainder of the Government.
- o Upon the implementation of the DOD hotline and any CIA rewards, ISOO should inform the remaining agencies of the status of these procedures. Further, it is recommended at the appropriate time that ISOO establish a "civilian" hotline of some type and that ISOO develop a proposal for establishing a system of rewards/awards for non-intelligence and non-defense Government employees for reporting unauthorized disclosures.

Implementation

The Task Force believes these recommendations, if adopted, should be coordinated by ISOO.

LIMITED OFFICIAL USE

Initiative

Revise investigative procedures and security inspections pertaining to unauthorized disclosures.

- o It is recommended that guidelines be issued to encourage agency and department internal investigations which develop leads or probable sources that can be turned over to the Federal Bureau of Investigation (FBI). The guidance would include information on what could and could not be done in an internal investigation.
- o It is also recommended that security inspections and compliance reviews be restructured to include items that could deter unauthorized disclosures. Examples of this could be the adherence to media contact procedures and whether there were adequate internal investigations of leaks.

Implementation

The Task Force proposes that the DOJ and the FBI develop a draft of new guideline for the departments and agencies on the internal investigations of leaks. The Task Force also proposes that ISOO issue guidelines for adoption by the departments on expanding compliance reviews to include procedures to reduce the number of unauthorized disclosures.

LIMITED OFFICIAL USE



Department of Energy
Washington, D.C. 20545

August 30, 1985

Mr. Steven Garfinkel
Director, Information Security
Oversight Office
6042 GSA Main Building
18th and F Street, NW
Washington, DC 20405

Dear Steve:

As you requested, enclosed is a copy of the DOE/DOD Task Force submission on overclassification. We have made every effort to be concise and to the point so that the overall report does not become too cumbersome. We have identified four initiatives altogether; two for each of the reasons for overclassification which we analyzed.

If you have any questions with regard to our submission, your staff should contact Joan Hawthorne (353-4338). I look forward to receiving the inputs from the other agency task forces.

Sincerely,

A handwritten signature in dark ink, appearing to read "Jill Ellman Lytle".

Jill Ellman Lytle
Director
Office of Classification

Enclosure

cc w/enclosure:
Britt Snyder, DOD
E. Theis, ISOO
B. Rich, DP-343.3

48/2

DOE/DOD TASK FORCE SUBMISSION: INITIATIVES FOR
REDUCING OVERCLASSIFICATION

Purpose

The purpose of this task force was to (1) analyze the primary reasons for overclassification; (2) select and define initiatives that would seek to reduce the problem of overclassification; and (3) recommend procedures for the implementation of the chosen initiatives.

The term "overclassification" in this instance refers to unnecessary classification. This task force did not address the issue of overgrading (e.g., Secret versus Confidential). However, it should be noted that the recommended initiatives could be applied to all forms of improper classification, including overgrading and underclassification.

Discussion

Classification is subjective in nature, and, as such, there is no way to ensure absolute consistency and accuracy in all classification decisions. It was the consensus of the task force that, in relative terms, overclassification was not a problem of immense proportions. However, it was recognized that a few well-publicized violations can have a very deleterious effect on the system as a whole, from the perspective of both those within it, and those on the outside. It is, therefore, a problem which should be reckoned with and avoided to the extent possible.

Numerous factors were considered in the evaluation of the reasons for overclassification. As these factors were evaluated, it became apparent that they could be reduced to two primary reasons: (1) Lack of knowledge (i.e., insufficient guidance and/or lack of specific enough guidance, and training); and (2) inadequate oversight.

A third reason that was surfaced, lack of sanctions for abuses, was dismissed on the basis that Executive Order 12356 adequately addresses this area. It was felt that the real weakness in the system arises in the lack of application of sanctions due to inadequate oversight.

On the basis of the two primary reasons for overclassification outlined above, four initiatives to reduce overclassification have been identified. These initiatives are discussed in the following attachments along with recommendations for procedures to implement them.

ISSUE: Lack of Classifier Knowledge

INITIATIVE #1

Establishment by the ISOO of minimal criteria for mandatory training for classifiers on original and derivative classification decisions and the use of guides.

DISCUSSION:

Adequate knowledge through education and training is critical to the achievement of accurate classification. While Executive Order 12356 mandates a "security education program to assure effective implementation of this Order," the Implementing Directive contains only broad guidelines: "The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings." Education and training programs vary widely among the agencies, and particular concerns have been raised with regard to the lack of training of senior agency officials. It is, therefore, proposed that the ISOO issue detailed minimal standards for the mandatory training of classifiers on original and derivative classification decisions and the use of classification guides. Particular emphasis should be placed on the training of senior agency personnel.

IMPLEMENTATION:

1. Have the ISOO draft detailed minimal standards required for training, including mandatory training for senior agency personnel.
2. Coordinate through agency review.
3. Publish the standards in an ISOO directive.

ISSUE: Lack of Classifier Knowledge

INITIATIVE #2

Establishment by the ISOO of (a) criteria for determining when formal written classification guidance is required; and (b) a handbook for preparing classification guidance (including formal guides and alternative methods, such as bulletins).

DISCUSSION:

Agencies are required to develop and issue classification guides for all classified areas within their jurisdiction unless it is determined by appropriate agency authority that such guides are not feasible. The degree of detail and the extent of coverage of such guides varies widely among the agencies and yet comprehensive and consistent classification guidance is essential for proper classification determinations. Agencies must ensure that offices or programs whose classified functions are not otherwise covered by classification guides are provided with guidance in sufficient detail that they can properly carry out their classified functions. To aid agencies in the development of such guidance, it is proposed that the ISOO issue criteria for determining whether formal classification guidance is required and, further, that the ISOO issue a handbook for preparing classification guidance. In particular, the handbook should address alternatives to "formal guides," e.g., bulletins, that would enable agencies to fulfill current guidance requirements and perhaps "tailor" their classification guidance for selected elements of their organizations.

IMPLEMENTATION:

1. Have the ISOO draft (a) criteria for determining when formal, written classification guidance is required, and (b) a handbook for preparing classification guidance (including formal guides and alternative methods, such as bulletins).
2. Coordinate through agency review.
3. Issue the criteria in an ISOO directive and publish the handbook for agency use.

ISSUE: Inadequate Oversight

INITIATIVE #3

Establishment by the ISOO of minimal criteria for agency self-inspections and ISOO inspections, including a mandate for each agency to sample its classified information for overclassification.

DISCUSSION:

While sanctions exist in the Executive Order to deter overclassification, they are generally not effective because there is insufficient oversight to identify instances of overclassification. Effective deterrence can only be achieved through self-inspections and monitoring programs. To assure adequate and consistent standards among the agencies, it is proposed that the ISOO develop a set of minimal criteria for agency self-inspections and ISOO inspections. Such criteria should include a mandate for each agency to sample its classified information for overclassification.

IMPLEMENTATION:

1. Have the ISOO draft a set of minimal standards for agency self-inspections and ISOO inspections.
2. Coordinate through agency review.
3. Publish the standards in an ISOO directive.

ISSUE: Inadequate Oversight

INITIATIVE #4

Provide an effective means for classification decisions to be challenged by those who believe a document is overclassified and, further, impose a requirement on all Executive Branch employees to challenge the classification of a document which comes into their authorized possession which they believe to be overclassified.

DISCUSSION:

A classification system that does not provide an effective mechanism for challenging decisions has an increased potential for improper classification determinations being made. It is believed that a well publicized challenge system, with assurances that employees who utilize such a system in good faith would not be subject to retaliation, could provide an additional means for deterring overclassification. Agencies could choose implementation alternatives suitable for their circumstances. One alternative might be the establishment of a classification review board where documents which were judged to be overclassified could be sent. Another alternative might be to establish a "hot line" to the senior agency official, or some other appropriate official in the agency, where complaints could be registered. With any of these mechanisms, the "senior official" or review board could be given authority to review any information classified by the agency, and to require the responsible official to justify the classification assigned a particular document. If such justification were lacking or insufficient, the "senior official" or board could be given authority to order the declassification of the information in question, subject to appeal to an appropriate agency official.

IMPLEMENTATION:

1. Have the ISOO draft a statement requiring agencies to (a) implement an effective method for allowing government employees to challenge classification decisions, and (b) impose a requirement on all government employees to challenge classification decisions they believe to be in error. Such a statement should include a requirement that agencies make these new policies well known to their employees and that assurances be given that employees who challenge classification decisions in good faith will not be subject to any form of retaliation.
2. Coordinate through agency review.
3. Publish the policy in an ISOO directive.



United States Department of State

Washington, D.C. 20520

August 27, 1985

Mr. Steven Garfinkel
Director
Information Security Oversight Office
Room 6046
18th & F Street, N.W.
Washington, D.C. 20405

Dear Steve:

In response to the request made at your interagency meeting of July 30, 1985 on Information Security Incentives, I have pleasure in enclosing a memorandum on the revitalizing of Need-to-Know which has been coordinated with the Department of Army Materiel Command.

Sincerely,

A handwritten signature in dark ink, appearing to read "J. R. Burke", with a long horizontal flourish extending to the right.

John R. Burke
Deputy Assistant Secretary
Classification/Declassification Center
Bureau of Administration and Security

Enclosure:
As stated.

Need-to-Know - Revitalizing

Objective

To minimize opportunities for leaks of sensitive information by strengthening application of the need-to-know principle.

Background

It is not always recognized that the granting of a security clearance does not automatically entitle a government employee to right of access to classified information. The employee must also have a need-to-know, defined in E.O. 12356 as "access (being) essential to the accomplishment of lawful and authorized government purposes."

While the current E.O. 12356 provides for sanctions against those who knowingly, willfully or negligently disclose properly classified information, it does not specifically make clear that "unauthorized persons" include those who, although holding an appropriate security clearance, do not also have a need-to-know.

Strict application of the need-to-know principle has

- 2 -

markedly declined, particularly when considered against its successful observance in the most crucial situations of WW II such as the Manhattan project and the protection of key invasion dates.

As a practical matter, it would be impossible, and generally unacceptable, to recreate such an atmosphere of crisis under peacetime conditions, but the relaxation in standards is due to a great variety of additional factors. These include overclassification in years gone by (no longer a serious problem), widespread sharing of information within and among agencies, facilitated by the huge proliferation of xerox machines and computerized data, a weakening of discipline at all levels, exemplified by leaks of every type of information from critical to trivial, the growing power of the media and their assumption of a right-to-know, rather than a need-to-know, and the trend towards openness as a government policy, embodied in statutes such as the FCIA.

Present Procedures

Partly, at least, in response to the weakening of the need-to-know principle, agencies have devised a wide variety of other in-house methods of control. To give one example, some agencies have created many "Special Access Programs (SAPs)," as

- 3 -

authorized by E.O. 12356, to control access to specially sensitive information. (In fact, the creation of SAPs has become, in many cases, an expensive substitute for the strict enforcement of "need-to-know.") Top secret documents are, of course, individually controlled by all agencies - an effective but very time consuming way to limit access and pinpoint responsibility. Nevertheless, very few agencies, if any, are so organized as to be able to enforce perfect application of the need-to-know principle. For most agencies, only certain components handling tightly limited bodies of information, e.g., permanent libraries of classified materials, can achieve complete control.

At present, the need-to-know criterion is, or should be, applied by the officer originating the classification, who also creates the distribution list for the document. However, in many instances subsequent distribution is made automatically by the communications office or other transmitting office on the basis of "tags" or of key words in the text, and receiving offices also freely copy documents and distribute them to other security-cleared personnel. It is almost unknown for distribution to be curtailed once the document has left the originating office, and much more common for it to be expanded.

- 4 -

Problems in Modifying Existing Procedures

Verification. Whatever method is adopted to tighten application of the need-to-know principle must take into account the difficulties of monitoring. The Department of Defense handles millions of pages of classified documents and hundreds of contractors cleared for access, and would find it absolutely impossible to administer an overall checking system through the life of a document. Further, it would be impossible for a lay inspector in a scientific or technical setting to determine which scientist or technician had a need-to-know. Even on a smaller scale, the task would be equally overwhelming for agencies such as State. There is also the problem of sensitive information discussed at formal and informal meetings, in daily office situations, etc. - it would border on the absurd to attempt to assess each participant's need-to-know. It would be yet another monumental task to key detailed need-to-know criteria into data retrieval systems.

Variation in Material. A great variety of national security information exists within a single classification. Top secret material relating, for example, to a weapons system can and should be restricted to a finite, fairly easily defined group, particularly in the research and development stage. But

- 5 -

top secret though fragmentary information relating to the intentions of a potential enemy and obtained from a sensitive source should probably be shared with a fairly wide group of intelligence analysts if it is to be fully, accurately evaluated. Thus careful balances must be struck in making distribution decisions on various types of sensitive information.

Recommendations

1) The original classifier must in the first instance remain as the official responsible for application of the need-to-know principle, but subsequent recipients of the information must also be alerted to their responsibilities in this regard. We propose a vigorous campaign, possibly initiated by a statement from the White House, under the general responsibility of ISOO but centered in the Senior Official in each agency, to remind all classifying officers of this aspect of their work, and all other security cleared employees of their responsibilities in further distribution. Such a campaign would include written notices, flyers, possibly posters and increased emphasis on need-to-know in security briefings. It would also include review of current distribution lists, including distributions made to other agencies, and of Special Access Programs.

- 6 -

2) For reasons given above, complete or even extensive monitoring of the application of need-to-know is not practicable and our main emphasis must be on the hortatory approach, but monitoring should be practiced as far as possible. Agencies which are able to control access to limited bodies of information should continue to do so and all agencies should examine their procedures to see if other limited area control can be achieved.

3) In addition, agencies should wherever possible establish a spot-checking procedure for documents, as is now carried out in many agencies to determine appropriateness of classification. This would be in addition to similar checks to be made by ISCO in the course of its normal inspections.

4) Some redrafting of E.O. 12356 and/or ISCO Directive No. 1 may be necessary in order to accommodate new procedures and legitimate concerns. We presume also that any modifications of current practice would be made in the context of NSDD-84, should that initiative be revived in its original form, though it appears unlikely that the two would conflict.



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO


5510
Ser 009P34/5U362946

29 AUG 1985

Director, Information Security Oversight Office
Attn: Mr. Steven Garfinkel
General Services Administration
18th & F Street, NW., Room 6042
Washington, DC 20405

Dear Mr. Garfinkel,

The enclosure is the report of the Classification Management Task Force. It has been coordinated with and concurred in by the Department of Treasury member and the ISOO liaison officer.


ROBERT C. ALLEN
Director, Security Policy Division
By the direction of the Chief of
Naval Operations

Copy to:
Department of Treasury (ATTN: Mr. Dennis Southern)

Encl:
(1) Report of the Classification Management Task Force



REPORT OF THE CLASSIFICATION MANAGEMENT TASK FORCE

The Classification Management Task Force was charged by The Director, Information Security Oversight Office (ISOO) to develop job performance standards for personnel engaged in classification management activities. This tasking is part of an ISOO effort to enhance overall security in the Executive Branch.

In approaching its assignment, the Task Force recognized the need to establish, as a first step, a basis from which job performance standards could be meaningfully developed. That is, first it would be necessary to establish functional descriptors for the classification management profession so that a position in this field could be clearly defined in all of its aspects. This would require Office of Personnel Management (OPM) revision of the GS-080 (security) position standards to include classification management as a functional specialization of the security field. Inasmuch as the GS-080 series has not been revised for more than twenty years, it would seem that the entire series could be revised to identify and describe the functional responsibilities of all other security specialties, such as ADP security, operations security (OPSEC), communications security (COMSEC), and so on, all of which are subsets of and can include aspects of information, personnel, and/or physical security.

It would follow, then, that once the security profession has been clearly described, each of its facets, including classification management, could be addressed from the perspective of training. We then would be able to prescribe training for personnel so that they may be trained to perform the functions described in the security standard(s). Once personnel are trained to perform required functions, it would be a relatively simple matter to develop performance standards against which employees may be judged as to how well, or how poorly they perform the described functions.

There is little formal training in security which is available to all agencies and departments. Individual agencies and departments have, to varying degrees, some ongoing training in specific areas of security. The DOD is currently expanding its Security Institute in Richmond, VA to accommodate a newly - adopted program of basic security instruction to cover all aspects of security for DOD personnel, both military and civilian.

From the foregoing, the Task Force recommends that:

1. The President direct OPM to revise the GS-080 series, ensuring that classification management and other security functional areas are addressed as separate areas of security specialization. Accomplishment of this effort will do much to ensure that suitable personnel are recruited and assigned to recognized security duties which will improve professionalism in the classification management field as well as in ancillary security areas.

2. The President direct the Secretary of Defense to explore the feasibility of expanding the Defense Security Institute (DSI) to provide basic security training to personnel throughout the Executive Branch on a cost - reimbursable basis. This training would be based on a modular curriculum so that personnel with responsibilities concentrated in one security area, i. e., information, physical, or personnel security, could be instructed primarily in their areas of interest.

Enclosure (1)

3. The President revise Executive Order 12356 to identify classification management as an area warranting agency head attention. The Order should define classification management and require that classification management be a factor in all military and civilian employee performance ratings for positions which involve access to classified information. As an alternative, ISOO could issue a directive to accomplish the same objective. The Task Force would define classification management as that functional element of Information Security which is concerned with the identification, classification, declassification, and marking of information to be safeguarded in the national interest pursuant to statute or Executive Order.

Central Intelligence Agency



Washington D C 20505

29 August 1985

Steven Garfinkel
Director, Information Security
Oversight Office (Z)
General Services Administration
18th & F Streets, N.W.
Washington, DC 20405

Dear Mr. Garfinkel:

In response to your request, the Central Intelligence Agency and the U. S. Air Force formed a joint task force to study the overdistribution of classified information in the Federal government.

Transmitted herewith are the findings and recommendations of that task force.

Sincerely,



Director of Information Services
Directorate of Administration

STAT

JOINT CIA U.S. AIR FORCE TASK FORCE
REPORT ON INITIATIVES TO REDUCE THE OVERDISTRIBUTION
OF CLASSIFIED PUBLICATIONS

Background:

In response to the request by the Director, Information Security Oversight Office (ISOO) to provide initiatives on reducing overdistribution of classified information within the Federal government, representatives of the Central Intelligence Agency and the U.S. Air Force formed a joint task force to review distribution procedures within their areas of responsibility and make recommendations to the Director, ISOO.

Based on guidance provided by the ISOO liaison representative, the task force focused its attention on the external distribution of publications. After reviewing the distribution procedures within their respective areas, the task force met on 20 August to discuss individual recommendations and to prepare a list of joint initiatives that might serve as a basis for resolving the overdistribution problem.

Based on the findings, the task force recommends the following initiatives:

Initiative No. 1

That Federal agencies be required to review the distribution of all classified publications and that originators and recipients meet periodically to update distribution lists and revalidate the recipients' need-to-know.

Implementation:

Incorporate into ISOO Directive No. 1, Section 2001.62, "Oversight" (32 CFR 2001.62)--or into a new section of the directive--a requirement for Agency heads to implement procedures for reviewing, on at least an annual basis, the distribution of all classified publications. Specifically, originators and recipients should be required to periodically meet and update their distribution lists to revalidate continuing substantive need and individual recipient need-to-know.

Initiative No. 2

Incorporate into the annual ISOO inspection program a review of the dissemination procedures for classified publications for both originating and receiving agencies.

Implementation:

Pursuant to Director, ISOO's authority under Executive Order 12356, Section 5.2(b)(4), include the review of dissemination procedures for classified publications in ISOO's annual inspection program.

Initiative No. 3

Establish a series of interagency seminars for both producers and consumers of classified publications. These seminars could serve to familiarize supervisors, analysts, and publication support specialists with the seriousness of overdistribution and to enlist their support in resolving this problem.

Implementation:

Pursuant to ISOO Directive No. 1, Section 2001.61, (32 CFR 2001.61) "Security Education", establish interagency seminars to make producers and consumers of classified publications aware of their responsibility to reduce excessive distribution of classified publications. The theme, "Overdistribution", should also be included in the next ISOO symposium.

STAT

29 Aug 85
Date

Agency Security Classification Officer
Central Intelligence Agency

29 Aug 85
Date

John P. Cornett
Chief, Information Security
Office of Security Police
Headquarters USAF
U.S. Air Force